# Cyberterrorism: Media Myth or Clear and Present Danger?

*Maura Conway*

## 1. Introduction

The Internet is the instrument of a political power shift. It is the first many-to-many communication system. The ability to communicate words, images, and sounds, which underlies the power to persuade, inform, witness, debate, and discuss (not to mention the power to slander, propagandise, disseminate bad or misleading information, engage in misinformation and/or disinformation, etc.) is no longer the sole province of those who own printing presses, radio stations, or television networks. Every machine connected to the Internet is potentially a printing press, a broadcasting station, a place of assembly. And in the twenty first century, terrorists are availing of the opportunity to connect.

The Internet is an ideal propaganda tool for terrorists: in the past they had to communicate through acts of violence and hope that those acts garnered sufficient attention to publicise the perpetrators cause or explain their ideological justification. With the advent of the Internet, however, the same groups can disseminate their information undiluted by the media and untouched by government sensors. In 1998 it was reported that 12 of the 30 terrorist organisations identified by the US State Department had their own websites. Today, a majority of the 33 groups on the same list of Designated Foreign Terrorist Organisations maintain an official online presence (see Conway 2002).[1] The question that then arises is this: Are terrorist groups who use the Internet in such a manner 'cyberterrorists'? The answer hinges on what constitutes cyberterrorism.

The term cyberterrorism unites two significant modern fears: fear of technology and fear of terrorism. Both of these fears are evidenced in this quote from Walter Laqueur, one of the most well known figures in terrorism studies: "The electronic age has now made cyberterrorism possible. A onetime mainstay of science fiction, the doomsday machine, looms as a real danger. The conjunction of technology and terrorism make for an uncertain and frightening future" (Laqueur 1999, 254). It is not only academics that are given to sensationalism. Cyberterrorism first became the focus of sustained analysis by government in the mid-1990s. In 1996 John Deutch, former director of the Central Intelligence Agency (CIA), testified before the Permanent Subcommittee on Investigations of the United States' Senate Governmental Affairs Committee:

> International terrorist groups clearly have the capability to attack the information infrastructure of the United States, even if they use relatively simple means. Since the possibilities for attacks are not difficult to imagine, I am concerned about the potential for such attacks in the future. The methods used could range from such traditional terrorist methods as a vehicle-delivered bomb -- directed in this instance against, say, a telephone switching centre or other communications node -- to electronic means of attack. The latter methods could rely on paid hackers. The ability to launch an attack, however, are likely to be within the capabilities of a number of terrorist groups, which themselves have increasingly used the Internet and other modern means for their own communications. The groups concerned include such well-known, long-established organizations as the Lebanese Hizballah, as well as nameless and less well-known cells of international terrorists such as those who attacked the World Trade Center (Deutch 1996).

It was Deutch who, in the same testimony, warned that an "electronic Waterloo" was a real possibility thus coining a neologism employed with startling frequency since.

In 1998 the Center for Strategic and International Studies, located in Washington DC, published their report entitled *Cybercrime, Cyberterrorism, Cyberwarfare: Averting an Electronic Waterloo*. The document's authors view cyberterrorism as a sub-species of Information Warfare (IW). And although they fail to provide a definition of what it is they mean by 'cyberterrorism,' they are at pains to illustrate its potentially disastrous consequences:

> A smoking keyboard does not convey the same drama as a smoking gun, but it has already proved just as destructive. Armed with the tools of Cyberwarfare, substate or nonstate or even individual actors are now powerful enough to destabilise and eventually destroy targeted states and societies… Information warfare specialists at the Pentagon estimate that a properly prepared and well-coordinated attack by fewer than 30 computer virtuosos strategically located around the world, with a budget of less than $10 million, could bring the United States to its knees. Such a strategic attack, mounted by a cyberterrorist group, either substate or nonstate actors, would shut down everything from electric power grids to air traffic control centers (CSIS 1998, xiii).

A focus on such 'shut-down-the-power-grid' scenarios is increasingly a feature of analyses of the cyberterrorist threat (see Devost, Houghton & Pollard 1996, 1997, also Pollitt n.d. & Benner 2001).

This chapter is concerned with the origins and development of the concept of cyberterrorism. It seeks to excavate the story of the concept through an analysis of both popular/media renditions of the term and scholarly attempts to define the borders of same. Let me say at the outset that, in both realms, confusion abounds. This is startling, particularly given that since the events of 9-11, the question on everybody's lips appears to be 'Is Cyberterrorism Next?' (Denning 2001a; Swartz 2001). In academic circles the answer is generally 'not yet.' The media are less circumspect, however, and policy makers appear increasingly to be seduced by the latter's version of events. It seems to me that both question and answer(s) are hampered by the lack of certainty surrounding the central term. Let me begin by putting forward some concrete illustrations of this definitional void culled from newspaper accounts.

## 2. Cyberterrorists Abound

In June 2001 a headline in the *Boston Herald* read 'Cyberterrorist Must Serve Year in Jail' (Richardson 2001). The story continued: "Despite a Missouri cyberterrorist's plea for leniency, a Middlesex Superior Court judge yesterday told the wheelchair-bound man 'you must be punished for what you've done' to Massachusetts schoolchildren and ordered him to serve a year in jail." Christian Hunold, 21, pleaded guilty to "launching a campaign of terror via the Internet" from his Missouri home, including directing Middle School students to child pornography Web sites he posted, telephoning threats to the school and to the homes of some children, and posting a picture of the school's principal with bullet holes in his head and chest on the Net.

In December 2001 a headline in the *Bristol Herald Courier*, Wise County, Virginia, USA read 'Wise County Circuit Court's Webcam "Cracked" by Cyberterrorists' (Still 2001). The webcam, which allows surfers to log on and watch the Wise County Circuit Courts in action, was taken offline for two weeks for repairs. "(Expletive Deleted) the United States Government" was posted on a web page, but the defaced page could only be seen by the Court's IT contractors. Internet surfers who logged on could only see a blank screen. The 'attack' is though to have originated in Pakistan or Egypt, according to the report. "This is the first cyberterrorism on the court's Internet technology, and it clearly demonstrates the need for constant vigilance," according to Court Clerk Jack Kennedy. "The damage in this case amounted to a $400 hard drive relating to the Internet video server. The crack attack has now resulted in better software and enhanced security to avoid a [*sic*] further cyberterrorism." According to Kennedy, cracking can escalate to terrorism when a person cracks into a government- or military-maintained Web site; he said cyberterrorism has increased across the United States since the events of 9-11 and law enforcement has traced many of the attacks to Pakistan and Egypt.[2]

The scare mongering is not confined to the US, however. In March 2002 British IT security specialists Digilog published what has been described as "the most comprehensive study of the insecurity of wireless networks in London" (Leyden 2002). The survey discovered that over 90 per cent of those networks are open to drive-by hacking. Unfortunately, this potentially worthwhile survey is undermined by the emphasis placed on the supposed link between drive-by hackers and international terrorism: "And networks are not only at risk from attacks at close quarters. University research in Hawaii has shown that signals can be intercepted from a distance of over 25 miles, raising fears of large-scale cyber-terrorism. Computer-controlled power grids, telephone networks and water-treatment plants are at risk" (as quoted in Leyden 2002; see also Boutin 2002).

Also in March linkLINE Communications, described as "a small, but determined Internet service provider" located in Mira Loma, California received telephone and e-mail threats from an unnamed individual who claimed to have accessed- or be able to access- the credit card numbers of linkLINE's customers. He said that he would sell the information and notify linkLINE's customers if $50,000 wasn't transferred to a bank account number that he supplied. The ISP refused to concede to the cracker's demands: "We're not going to let our customers, or our reputation, be the victims of cyber-terrorism," said one of the company's founders. linkLINE contacted the authorities and learned that the cracker and his accomplices may have extorted as much as $4 billion from other companies. The account was subsequently traced through Russia to Yemen (linkLINE Communications Inc. 2002).

A similar incident had taken place in November 2000. An attack, originating in Pakistan, was carried out against the American Israel Public Affairs Committee, a lobbying group. The group's site was defaced with anti-Israeli commentary.[3] The attacker also stole some 3,500 e-mail addresses and 700 credit card numbers, sent anti-Israeli diatribes to the addresses and published the credit card data on the Internet. The Pakistani hacker who took credit for the crack, the self-styled Dr. Nuker, said he was a founder of the Pakistani Hackerz Club, the aim of which was to "hack for the injustice going around the globe, especially with [*sic*] Muslims" (Schwartz 2000).

In May 2001 'cyberterrorism' reared its head once again when supporters of the terrorist group Laskar Jihad (Holy War Warriors) hacked into the websites of the Australian embassy and the Indonesian national police in

Jakarta to protest against the arrest of their leader. The hackers intercepted users logging on to the Web sites and redirected them to a site containing a warning to the Indonesian police to release Ja'far Umar Thalib, the group's leader. Thalib was arrested in connection with inciting hatred against a religious group and ordering the murder of one of his followers. According to police, the hackers, the self-styled Indonesian Muslim Hackers Movement, did not affect police operations. The Australian embassy said the hackers did not sabotage its Web site, but only directed users to the other site (Anonymous 2001).

It is clear that the pejorative connotations of the terms 'terrorism' and 'terrorist' have resulted in some unlikely acts of computer abuse being labelled 'cyberterrorism'. According to the above, sending pornographic e-mails to minors, posting offensive content on the Internet, defacing Web pages, using a computer to cause $400 worth of damage, stealing credit card information, posting credit card numbers on the Internet, and clandestinely redirecting Internet traffic from one site to another all constitute instances of cyberterrorism. And yet none of it could be described as terrorism - some of it not even criminal - had it taken place without the aid of computers. Admittedly, terrorism is a notoriously difficult activity to define; however, the addition of computers to plain old criminality it is not.

## 3. What is Cyberterrorism?

There are a number of stumbling blocks to constructing a clear and concise definition of cyberterrorism. Chief among these are the following:

(a.) A majority of the discussion of cyberterrorism has been conducted in the popular media, where the focus is on ratings and readership figures rather than establishing good operational definitions of new terms.

(b.) The term is subject to chronic misuse and overuse and since 9/11, in particular, has become a buzzword that can mean radically different things to different people.

(c.) It has become common when dealing with computers and the Internet to create new words by placing the handle *cyber*, *computer*, or *information* before another word. This may appear to denote a completely new phenomenon, but often it does not and confusion ensues.

(d.) Finally, a major obstacle to creating a definition of cyberterrorism is the lack of an agreed-upon definition of terrorism (Embar-Seddon 2002, 1034).

This does not mean that no acceptable definitions of cyberterrorism have been put forward. On the contrary, there are a number of well thought out definitions of the term available, and these are discussed below.[4] However, no single definition of cyberterrorism is agreed upon by all, in the same way that no single, globally accepted definition of classical political terrorism exists.

Barry Collin, a senior research fellow at the Institute for Security and Intelligence in California, coined the term 'cyberterrorism' in the 1980s. The concept is composed of two elements: cyberspace and terrorism. Cyberspace may be conceived of as "that place in which computer programs function and data moves" (Collin 1996). Terrorism is a less easily defined term. In fact, most scholarly texts devoted to the study of terrorism contain a section, chapter, or chapters devoted to a discussion of how difficult it is to define the term (see Gearty 1991; Guelke 1998; Hoffman 1998; Holms 1994; Schmid & Jongman 1988; Wardlaw 1982). This chapter employs the definition of terrorism contained in Title 22 of the United States Code, Section 2656f(d).[5] That statute contains the following definition:

> The term 'terrorism' means premeditated, politically motivated violence perpetrated against non-combatant targets by sub-national groups or clandestine agents, usually intended to influence an audience."

Combining these definitions results in the construction of a narrowly drawn working definition of cyberterrorism as follows:

> cyberterrorism refers to premeditated, politically motivated attacks by sub-national groups or clandestine agents against information, computer systems, computer programs, and data that result in violence against non-combatant targets (Pollitt n.d.).

The above definition is similar to that put forward by Professor Dorothy Denning in numerous articles and interviews, and in her testimony before the United States Congress's House Armed Services Committee (Denning 2002, 2000a, 2000b, 1999). According to Denning:

> Cyberterrorism is the convergence of cyberspace and terrorism. It refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to

> intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.

Utilising these definitions, the 'attack' on the Web-cam of the Wise County Circuit Court does not qualify as cyberterrorism, nor do any of the other 'cyberterrorist attacks' outlined. It's hardly surprising; the inflation of the concept of cyberterrorism may increase newspaper circulation, but is ultimately not in the public interest. Despite this, many have suggested adopting broader definitions of the term.

In an article, which appeared in the journal *Terrorism and Political Violence* in 1997, Devost, Houghton and Pollard defined 'information terrorism' as "the intentional abuse of a digital information system, network or component toward an end that supports or facilitates a terrorist campaign or action" (1997, 75). They conceive of information terrorism as "the nexus between criminal information system fraud or abuse, and the physical violence of terrorism" (1996, 10; 1997, 76). This allows for attacks that would not necessarily result in violence against humans - although it might incite fear - to be characterised as terrorist. This is problematic because, although there is no single accepted definition of terrorism, more than 80% of scholars agree that the latter has two integral components: the use of force or violence and a political motivation (Guelke 1998, 19; Schmid & Jongman 1988, 5). Indeed, most domestic laws define classical or political terrorism as requiring violence or the threat to or the taking of human life for political or ideological ends. Devost, Houghton and Pollard are aware of this, but wish to allow for the inclusion of pure information system abuse (i.e. that does not employ nor result in physical violence) as a possible new facet of terrorism nonetheless (1996, 10). Others have followed their lead.

Israel's former science minister, Michael Eitan, has deemed "sabotage over the Internet" as cyberterrorism (Sher 2000). According to the Japanese government 'Cyberterrorism' aims at "seriously affecting information systems of private companies and government ministries and agencies by gaining illegal access to their computer networks and destroying data" (FBIS 2002b). A report by the Moscow-based ITAR-TASS news agency states that, in Russia, cyberterrorism is perceived as "the use of computer technologies for terrorist purposes" (FBIS 2002a). In 1999, a report by the Center for the Study of Terrorism and Irregular Warfare (CSTIW) at the Naval Postgraduate School in Monterey, California, defined cyberterrorism as the "unlawful destruction or disruption of digital property to intimidate or coerce people" (Daukantas 2001). "We shall define cyberterrorism as any act of terrorism…that uses information systems or computer technology either as a *weapon* or a *target*," states a NATO brief (Mates 2001, 6). Yael Shahar, Web master at the International Policy Institute for Counter-Terrorism (ICT), located in Herzliya, Israel, differentiates between a number of different types of what he prefers to call 'information terrorism': 'electronic warfare' occurs when hardware is the target, 'psychological warfare' is the goal of inflammatory content, and it is only 'hacker warfare', according to Shahar, that degenerates into cyberterrorism (Hershman 2000).

John Leyden, writing in *The Register*, described the way in which a group of Palestinian hackers and sympathisers established a Web site that provides one-stop access to hacking tool and viruses, and tips on how to use the tools to mount attacks on Israeli targets. They are, he said, using the techniques of cyberterrorism (Leyden 2000). Leyden and others wish to conflate politically motivated hacking - so-called hacktivism - and terrorism. Such unwarranted expansion of the concept of cyberterrorism runs contrary to the definitions outlined earlier. Advancing one step further, Johan J. Ingles-le Noble, writing in *Jane's Intelligence Review*, had this to say:

> Cyberterrorism is not only about damaging systems but also about intelligence gathering. The intense focus on 'shut-down-the-power-grid' scenarios and tight analogies with physically violent techniques ignore other more potentially effective uses of IT in terrorist warfare: intelligence-gathering, counter-intelligence and disinformation (1999, 6).

Noble's comment highlights the more potentially realistic and effective uses of the Internet by terrorist groups (i.e. intelligence-gathering, counter-intelligence, disinformation, etc.). However, he mistakenly labels these alternative uses 'cyberterrorism.' Such a taxonomy is uncalled for: even had Dr. Nuker broken into the headquarters of the American Israel Public Affairs Committee and physically stolen the credit card information and e-mail addresses, this would not be considered an act of terrorism, but a criminal undertaking. It is only acting on the information obtained to perpetrate an attack in furtherance of some political aim that could be considered terrorist. Noble contends, furthermore, that "disinformation is easily spread; rumours get picked up by the media, aided by the occasional anonymous e-mail." That may be so, but spreading false information whether via word-of-mouth, the print or broadcast media, or some other medium, is oftentimes not even criminal, never mind terrorist. Why should things be any different in cyberspace?

In fact, Ingles-le Noble (1999) himself recognises that:

> There is undoubtedly a lot of exaggeration in this field. If your system goes down, it is a lot more interesting to say it was the work of a foreign government rather than admit it was due to an American teenage 'script-kiddy' tinkering with a badly written CGI script. If the power goes out, people light a candle and wait for it to return, but do not feel terrified. If their mobile phones switch off, society does not instantly feel under attack. If someone cracks a web site and changes the content, terror does not stalk the streets.

Nonetheless, there is widespread concern that a catastrophic cyberterrorist attack is imminent particularly in the wake of the events of 9/11. However, the bulk of the evidence to date shows that while terrorist groups are making widespread use of the Internet, so far they have not resorted to cyberterrorism, or shown the inclination to move heavily in that direction. Dramatic predictions to the contrary certainly make good copy, generate high ratings and sell many books and journals, but do not contribute to an intelligent, well-informed analysis of the threat of cyberterrorism. Unfortunately, such predictions appear to have had a significant impact in policy circles. It has been observed that "there is a lot of fear around and perhaps governments are in possession of the most of it" (Stanton 2002, 1020). These inchoate fears have led to the introduction of a raft of legislation that, in many instances, fails to distinguish between both crime and terrorism, and malicious hacking and cyberterrorism. This sets a dangerous precedent.

## 4. Distinguishing Characteristics

When it comes to discussion of cyberterrorism, there are two basic areas in which clarification is needed. First, the confusion between cyberterrorism and cybercrime. Such confusion is partly caused by the lack of clear definitions of the two phenomena. A UN manual on IT-related crime recognises that, even after several years of debate among experts on just what constitutes cybercrime and what cyberterrorism, "there is no internationally recognised definition of those terms" (Mates 2001). Second, it is useful to distinguish two different facets of terrorist use of information technology: terrorist use of computers as a facilitator of their activities, and terrorism involving computer technology as a weapon or target. Utilising the definitions outlined above, it is possible to clarify both difficulties. Cybercrime and cyberterrorism are not coterminous. Cyberspace attacks must have a 'terrorist' component in order to be labelled cyberterrorism. The attacks must instil terror as commonly understood (that is, result in death and/or large-scale destruction), and they must have a political motivation. As regards the distinction between terrorist use of information technology (i.e. for the purposes of inter-group communication, propaganda, etc.) and terrorism involving computer technology as a weapon/target, only the latter may be defined as cyberterrorism. Terrorist 'use' of computers as a facilitator of their activities, whether for propaganda, communication, or other purposes, is simply that: 'use.'

Kent Anderson[7] has devised a three-tiered schema for categorising fringe activity on the Internet, utilising the terms 'Use,' 'Misuse,' and 'Offensive Use.' Anderson explains:

> Use is simply using the Internet/WWW to facilitate communications via e-mails and mailing lists, newsgroups and websites. In almost every case, this activity is simply free speech…Misuse is when the line is crossed from expression of ideas to acts that disrupt or otherwise compromise other sites. An example of misuse is Denial-of-Service (DoS) attacks against websites. In the physical world, most protests are allowed, however, [even] if the protests disrupt other functions of society such as train service or access to private property…The same should be true for online activity. Offensive use is the next level of activity where actual damage or theft occurs. The physical world analogy would be a riot where property is damaged or people are injured. An example of this type of activity online is the recent attack on systems belonging to the world economic forum, where personal information of high profile individuals was stolen (Weisenburger 2001, 2).

Combining Anderson's schema with the definition of cyberterrorism I outlined above it is possible to construct a four-level scale of the uses of the Internet for political activism by unconventional actors, ranging from 'Use' at one end of the spectrum to 'Cyberterrorism' at the other (see Table 1). Unfortunately, such a schema has not generally been employed in the literature or in the legislative arena. This is particularly disquieting given that the vast majority of terrorist activity on the Internet is limited to 'Use.'

**Table 1. Typology of Cyber Activism and Cyber Attacks**

| *Action* | *Definition* | *Source* | *Example* |
|---|---|---|---|
| *Use* | Using the Internet to facilitate the expression of ideas and communication(s) | Internet users | Emails, mailing lists, newsgroups, websites |
| *Misuse* | Using the Internet to disrupt or compromise Web sites or infrastructure | Hackers, Hacktivists | Denial-of-Service (DoS) attacks |
| *Offensive Use* | Using the Internet to cause damage or engage in theft | Crackers | Stealing data (e.g. credit card details) |
| *Cyberterrorism* | An attack carried out by terrorists either via the Internet or targeting the Internet that results in violence against persons or severe economic damage | Terrorists | A terrorist group using the Internet to carry out a major assault on the New York Stock Exchange |

## 5. Legislative Measures

In February 2001, the UK updated its Terrorism Act to classify "the use of or threat of action that is designed to seriously interfere with or seriously disrupt an electronic system" as an act of terrorism (see Di Maio 2001; Mates 2001).[6] In fact, it will be up to police investigators to decide whether an action is to be regarded as terrorism. Online groups, human rights organisations, civil liberties campaigners, and others condemned this classification as absurd, pointing out that it placed hacktivism on a par with life-threatening acts of public intimidation (Weisenburger 2001, 9).[8] Notwithstanding, in the wake of the events of 9-11, US legislators followed suit. Previous to 9/11, if one successfully infiltrated a federal computer network, one was considered a hacker. However, following the passage of the PATRIOT Act,[9] which authorised the granting of significant powers to law enforcement agencies to investigate and prosecute potential threats to national security, there is the potential for hackers to be labelled cyberterrorists and, if convicted, to face up to 20 years in prison (NIPC 2001; see also Middleton 2002 & Levin 2002, 984-985). Clearly, policymakers believe that actions taken in cyberspace are qualitatively different from those taken in the 'real' world.

It is not the PATRIOT Act, however, but the massive 500-page law establishing the US Department of Homeland Security that has the most to say about terrorism and the Internet. The law establishing the new department envisions a far greater role for the United States' government in the securing of operating systems, hardware, and the Internet in the future. In November 2002, US President Bush signed the bill creating the new department, setting in train a process which will result in the largest reshuffle of US bureaucracy since 1948. At the signing ceremony, Bush said that the "department will gather and focus all our efforts to face the challenge of cyberterrorism" (as quoted in McCullagh 2002). The Department of Homeland Security merges five agencies that shared responsibility for critical infrastructure protection in the United States: the FBI's National Infrastructure Protection Center (NIPC), the Defense Department's National Communications System, the Commerce Department's Critical Infrastructure Office, the Department of Energy's analysis center, and the Federal Computer Incident Response Center. The new law also creates a Directorate for Information Analysis and Infrastructure Protection whose task it will be to analyse vulnerabilities in systems including the Internet, telephone networks, and other critical infrastructures, and orders the establishment of a "comprehensive national plan for securing the key resources and critical infrastructure of the United States" including information technology, financial networks, and satellites. Further, the law dictates a maximum sentence of life-imprisonment without parole for those who deliberately transmit a program, information, code, or command that impairs the performance of a computer or modifies its data without authorisation, "if the offender knowingly or recklessly causes or attempts to cause death." In addition, the law allocates $500 million for research into new technologies, is charged with funding the creation of tools to help state and local law enforcement agencies thwart computer crime, and classifies certain activities as new computer crimes (Krebs 2002; McCullagh 2002; Poulsen 2002).

## 6. Conclusion

In the space of thirty years, the Internet has metamorphosed from a US Department of Defense command-and-control network consisting of less than one hundred computers to a network that criss-crosses the globe: today, the Internet is made up of tens of thousands of nodes (i.e. linkage points) with over 105 million hosts spanning more than 200 countries. With a current (December 2002) estimated population of regular users of over 600 million people, the Internet has become a near-ubiquitous presence in many world regions. That ubiquity is due in large part to the release in 1991 of the World Wide Web. In 1993 the Web consisted of a mere 130 sites, by century's end it boasted more than one billion. In the Western world, in particular, the Internet has been extensively integrated into the economy, the military, and society as a whole. As a result, many people now believe that it is possible for people to die as a direct result of a cyberterrorist attack and that such an attack is imminent.

On Wednesday morning, 12 September 2001, you could still visit a Web site that integrated three of the wonders of modern technology: the Internet, digital video, and the World Trade Center. The site allowed Internet users worldwide to appreciate what millions of tourists have delighted in since Minoru Yamasaki's architectural wonder was completed in 1973: the glorious 45-mile view from the top of the WTC towers. According to journalists, the caption on the site still read 'Real-Time Hudson River View from World Trade Center.' In the square above was deep black nothingness. The terrorists hadn't taken down the Net, they had taken down the towers. "Whereas hacktivism is real and widespread, cyberterrorism exists only in theory. Terrorist groups are using the Internet, but they still prefer bombs to bytes as a means of inciting terror," wrote Dorothy Denning (2001b) just weeks before the September attacks. Terrorist 'use' of the Internet has been largely ignored, however, in favour of the more headline-grabbing 'cyberterrorism.'

Richard Clarke, White House special adviser for Cyberspace Security, has said that he prefers not to use the term 'cyberterrorism,' but instead favours use of the term 'information security' or 'cyberspace security.' This is because, Clarke has stated, most terrorist groups have not engaged in information warfare (read 'cyberterrorism'). Instead, he admits, terrorist groups have at this stage only used the Internet for propaganda, communications, and fundraising (Wynne 2002). In a similar vein, Michael Vatis, former head of the US National Infrastructure Protection Center (NIPC), has stated that "Terrorists are already using technology for sophisticated communications and fund-raising activities. As yet we haven't seen computers being used by these groups as weapons to any significant degree, but this will probably happen in the future" (Veltman 2001). According to a 2001 study, 75% of Internet users worldwide agree, they believe that 'cyberterrorists' will "soon inflict massive casualties on innocent lives by attacking corporate and governmental computer networks." The survey, conducted in 19 major cities around the world, found that 45% of respondents agreed completely that "computer terrorism will be a growing problem," and another 35% agreed somewhat with the same statement (Poulsen 2001). The problem certainly can't shrink much, hovering as it does at zero cyberterrorism incidents per year. That's not to say that cyberterrorism cannot happen or will not happen, but that, contrary to popular perception, it has not happened yet.

## Notes

1. The European Union (EU) has recently updated its list of prohibited organisations (see http://ue.eu.int/pressData/en/misc/70413.pdf). Canada is the latest country to establish such a list ( see http://www.sgc.gc.ca/publications/news/20020723_e.asp).

2. It was predicted that an escalation in hack attacks would occur in the aftermath of 9-11 (ISTS 2001). However, the predicted escalation did not materialise. In the weeks following the attacks, Web page defacements were well publicised, but the overall number and sophistication of these remained rather low. One possible reason for the non-escalation of attacks could be that many hackers- particularly those located in the US- were wary of being associated with the events of September 11th and curbed their activities as a result.

3. The defacement may be viewed online at http://www.attrition.org/mirror/attrition/2000/11/02/www.aipac.org/.

4. One of the most accessible sound bites on what defines cyberterrorism is that it is 'hacking with a body count' (Collin, quoted in Ballard *et al* 2002, 992).

5. Title 22 of the United States Code, Section 2656f(d) may be viewed online at http://www.lii.warwick.ac.uk/uscode/22/2656f.html. This is the definition employed in the US State Department's annual report entitled *Patterns of Global Terrorism*. These are available online at http://www.state.gov.

6. The full text of the UK Terrorism Act 2001 is available online at http://www.legislation.hmso.gov.uk/acts/acts2000/20000011.htm.

7. Anderson was formerly senior vice-president of IT Security and Investigations for information security firm Control Risks Group.

8. Furthermore, ISPs in the UK may be legally required to monitor some customers' surfing habits if requested to do so by the police under the Regulation of Investigatory Powers Act 2000.

9. The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 was signed into law by US President George Bush in October 2001. The law gives government investigators broad powers to track wireless phone calls, listen to voicemail, intercept e-mail messages and monitor computer use, among others. I cannot enter into a discussion of the Act here due to limitations of space. However, the full text of the Act is available at http://www.ins.usdoj.gov/graphics/lawsregs/patriot.pdf (Section 1016 pertains to critical infrastructure protection). See also Johnson 2001; Matthews 2001.

**References**

Anonymous (2001), 'Hackers Divert Indonesian Hits', *The Age*, May 10. Available on the Internet at http://www.theage.com.au/news/2001/05/10/FFXTYW2ZHMC.html.

Ballard, J.D., J.G. Hornik, & D. McKenzie (2002). 'Technological Facilitation of Terrorism: Definitional, Legal and Policy Issues', *American Behavioral Scientist* 45(6): 989-1016.

Benner, Caroline (2001), 'The Phantom Cyber-Threat', *Salon*, April 4. Available on the Internet at http://www.salon.com/tech/feature/2001/04/04/cyberterrorism/print.html.

Boutin, P. (2002), 'Feds Label Wi-Fi a Terrorist Tool,' *Wired*, December 6. Available on the Internet at http://www.wired.com/news/wireless/0,1382,56742,00.html.

Center for Strategic and International Studies (CSIS), (1998), *Cybercrime, Cyberterrorism, Cyberwarfare: Averting an Electronic Waterloo*. Washington DC: CSIS.

Collin, B. (1996), 'The Future of Cyberterrorism', presented at the 11th Annual International Symposium on Criminal Justice Issues, University of Illinois at Chicago. Available on the Internet at http://www.afgen.com/terrorism1.html.

Conway, M. (2002), 'Reality Bytes: Cyberterrorism and Terrorist "Use" of the Internet', *First Monday* 7(11). Available on the Internet at http://www.firstmonday.org/issues/issue7_11/conway/index.html

Daukantas, P. (2001), 'Professors Hash Out Emergency Response, Cyberterrorism Strategies', *Government Computer News*, December 14. Available on the Internet at http://www.gcn.com/vol1_no1/daily-updates/17642-1.html.

Denning, D. (2001a), *Is Cyber Terror Next?* New York: US Social Science Research Council. Available on the Internet at http://www.ssrc.org/sept11/essays/denning.htm.

Denning, D. (2001b), 'Hacker Warriors: Rebels, Freedom Fighters, and Terrorists Turn to Cyberspace', *Harvard International Review*, Summer. Available on the Internet at: http://www.hir.harvard.edu/archive/articles/pdf/denning.html.

Denning, D. (2000a), *Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives*, May 23. Available on the Internet at http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html.

Denning, D. (2000b), 'Cyberterrorism', *Global Dialogue*, Autumn. Available on the Internet at http://www.cs.georgetown.edu/~denning/infosec/cyberterror-GD.doc.

Denning, D. (1999), *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*. Available on the Internet at: http://www.nautilus.org/info-policy/workshop/papers/denning.html.

Deutch, J. (1996), *Statement Before the US Senate Governmental Affairs Committee* (Permanent Subcommittee on Investigations), June 25. Available on the Internet at http://www.nswc.navy.mil/ISSEC/Docs/Ref/InTheNews/fullciatext.html.

Devost, M., B. Houghton & N. Pollard (1997), 'Information Terrorism: Political Violence in the Information Age', *Terrorism and Political Violence*, 9(1): 72-83.

Devost, M., B. Houghton & N. Pollard (1996), 'Information Terrorism: Can You Trust Your Toaster?', *The Terrorism Research Centre*. Available on the Internet at: http://www.terrorism.com/terrorism/itpaper.html.

Di Maio, P. (2001), 'Hacktivism, Cyberterrorism or Online Democracy?', *The Information Warfare Site (IWS)*, March 19. Available on the Internet at http://www.iwar.org.uk/hackers/resources/hacktivism-europe/internet-europe.htm.

Embar-Seddon, A. (2002). 'Cyberterrorism: Are We Under Siege?', *American Behavioral Scientist*, 45(6): 1017-1043.

Foreign Broadcast Information Service (FBIS) (2002a) 'Russia Cracks Down on 'Cyberterrorism'', *ITAR-TASS*, FBIS-SOV-2002-0208, February 8.

Foreign Broadcast Information Service (FBIS) (2002b), 'Government Sets Up Anti-Cyberterrorism Homepage', *Sankei Shimbun*, FBIS-EAS-2002-0410, April 10.

Gearty, C. (1991), *Terror*. London: Faber & Faber.

Guelke, A. (1998), *The Age of Terrorism and the International Political System*. London & New York: IB Tauris Publishers.

Havely, J. (2000), 'When States go to Cyber-War', *BBC News Online*, February 16. Available on the Internet at http://news.bbc.co.uk/hi/english/sci/tech/newsid_642000/642867.stm.

Hershman, T. (2000), 'Cyberterrorism is Real Threat, Say Experts at Conference', *Israel.internet.com*, December 11.

Hoffman, B. (1998), *Inside Terrorism*. London: Indigo.

Holms, J. (1994), *Terrorism*. New York: Windsor Publishing Corps.

Ingles-le Noble, J. (1999), 'Cyberterrorism Hype', *Jane's Intelligence Review*. Available on the Internet at http://www.iwar.org.uk/cyberterror/resources/janes/jir0525.htm.

Institute for Security Technology Studies (ISTS) (2001*), Cyber Attacks During the War on Terrorism: A Predictive Analysis*. Dartmouth College: Institute for Security Technology Studies. Available on the Internet at http://www.ists.dartmouth.edu/ISTS/counterterrorism/cyber_attacks.htm.

Johnson, B. (2001), 'Farewell Web Freedom?', *The Guardian* (UK), October 22.

Krebs, B. (2002), 'Homeland Security Bill Heralds IT Changes', *The Washington Post*, November 25. Available on the Internet at http://www.washingtonpost.com/wp-dyn/articles/A54872-2002Nov14.html.

Laqueur, W. (1999), *The New Terrorism: Fanaticism and the Arms of Mass Destruction*. Oxford: Oxford University Press.

Levin, B. (2002), 'Cyberhate: A Legal and Historical Analysis of Extremists' Use of Computer Networks in America', *American Behavioral Scientist* 45(6): 958-988.

Leyden, J. (2002), 'Drive-By Hacking Linked to Cyberterror', *The Register*, March 27. Available on the Internet at http://www.theregister.co.uk/content/55/24611.html.

Leyden, J. (2000), 'Palestinian Crackers Give Out Tools to Attack Israelis', *The Register*, December 4. Available on the Internet at http://www.theregister.co.uk/content/6/15199.html.

linkLINE Communications, Inc. (2002), 'linkLINE Communications Thwarts Cyber-Terrorist', *Yahoo!Finance*, March 19.

Mates, M. (Rapporteur) (2001), *Technology and Terrorism*. Brussels: NATO. Available on the Internet at http://www.tbmm.gov.tr/natopa/raporlar/bilim%20ve%20teknoloji/AU%20121%20STC%20Terrorism.htm.

Matthews, W. (2001), 'Anti-Terror Law Expands Powers,' *Federal Computer Week*, October 29. Available on the Internet at http://www.fcw.com/fcw/articles/2001/1022/web-terror-10-26-01.asp.

McCullagh, D. (2002), 'Bush Signs Homeland Security Bill', *CNET News*, November 25. Available on the Internet at http://news.com.com/2102-1023-975305.html.

Middleton, J. (2002), 'US Hackers Could Face Life Sentences', *Vnunet.com*, February 28. Available on the Internet at http://vnunet.com/News/1129590.

National Infrastructure Protection Center (NIPC) (2001), *NIPC Daily Report*, December 11.

Pollitt, M. (n.d.), *Cyberterrorism: Fact or Fancy?* Washington DC: FBI Laboratory. Available:http://www.cs.georgetown.edu/~denning/infosec/pollitt.html.

Poulsen, K. (2002), 'Lawyers Fear Misuse of Cyber Murder Law', *SecurityFocus Online*, November 21. Available on the Internet at http://online.securityfocus.com/news/1702.

Poulsen, K. (2001), 'Cyber Terror in the Air', *SecurityFocus.com*, June 30. Available on the Internet at http://www.businessweek.com/technology/content/jul2001/tc20010726_694.htm.

Richardson, F. (2001), 'Cyberterrorist Must Serve Year in Jail', *Boston Herald*, June 6.

Schmid, A. & A. Jongman (1988), *Political Terrorism: A New Guide to Actors, Authors, Concepts, Databases, Theories and Literature*. Amsterdam: North-Holland Publishing Company.

Schwartz, J. (2000), 'When Point and Shoot Becomes Point and Click', *The New York Times*, November 12.

Sher, H. (2000), 'Cyberterror Should be International Crime- Israeli Minister', *Newsbytes*, November 10.

Stanton, J.J. (2002), 'Terror in Cyberspace: Terrorists Will Exploit and Widen the Gap Between Governing Structures and the Public', *American Behavioral Scientist* 45(6): 1017-1032.

Still, K. (2001), 'Wise County Circuit Court's Webcam 'Cracked' by Cyberterrorists', *Bristol Herald Courier*, December 20.

Swartz, J. (2001), 'Experts: Cyberspace Could Be Next Target', *USA Today*, October 16.

Veltman, C. (2001), 'Beating Cyber Crime', *The Daily Telegraph* (UK), March 1: 12E.

Wardlaw, G. (1982), *Political Terrorism: Theory, Tactics, and Countermeasures*. Cambridge: Cambridge University Press.

Weisenberger, K. (2001), 'Hacktivists of the World, Divide', *SecurityWatch.com*, April 23. Available on the Internet at: http://www.securitywatch.com/TRE/042301.html.

Wynne, J. (2002), 'White House Advisor Richard Clarke Briefs Senate Panel on Cybersecurity', *Washington File*, February 14. Available on the Internet at http://usinfo.state.gov/topical/global/ecom/02021401.htm.